App. No. 10/734,846   Docket JP920030198US1
Filing Date: 12/12/2003

REMARKS

1. Posture of the case.

Claims 1-35 were originally filed. The present Office action of February 22, 2007 is a
first Office action.

2. Non-Prior Art Rejections

The February 22, 2007, Office action rejected claims 18-35 under 35 U.S.C. 101 on
grounds that the invention claimed therein was directed to non-statutory subject matter.
Applicant herein amends the claims to overcome the rejection.

As amended herein above, claims 18-26 are limited to functional descriptive material
claimed in combination with an appropriate computer readable medium to enable the
functionality to be realized. That is, the password generation program of claims 18-26 is limited
to a computer system. Claims 18-26 produce a useful, concrete and tangible result. That is, the
password generation program of claims 18-26 provides a password for a user based on an
application name without the user having to remember a password associated with an application
name.

As amended herein above, claim 27 is limited to a process, machine, manufacture, or a
composition of matter. That is, the computer program product of claim 27 comprises a *storage
medium* readable by a computer, wherein the specification makes it clear that this term is
different than the objected to "transmission medium." Present application, page 15, lines 25-31
("The term "computer readable medium" as used herein refers to any *storage* or transmission
medium that participates in providing instructions and/or data to the computer system 400 for
execution and/or processing. Examples of *storage media* include floppy disks, magnetic tape,
CD-ROM, a hard disk drive, a ROM or integrated circuit, a magneto-optical disk, or a computer
readable card such as a PCMCIA card and the like, whether or not such devices are internal or
external of the computer module 401.")

No new matter is added in the amendments to claims 18-27 since the specification as
originally submitted provides support. Present application, page 15, lines 1-14 (regarding a
computer system comprising a processor and a storage device connected to the processor); page
1, lines 23-26 (regarding generation program providing a password for a user based on an

App. No. 10/734,846   Docket JP920030198US1
Filing Date: 12/12/2003

application name without the user having to remember a password associated with an application name);   page 15, lines 25-31 (regarding "storage medium").

3. Prior Art Rejections

Claim 1-5, 10-12, 15, 18-22, 26-31 and 35 stand rejected under 35 U.S.C. 102(a) as being anticipated by U.S. Patent 5,592,553 (Guski). Claim 6-9, 13, 14, 16, 17, 23-26, 32-35 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Guski et al. (U.S. Patent # 5,592,553) in view of well-known practices in the art. Applicant herein amends claims to overcome the rejection.

General remarks

Guski teaches password generation and evaluation in the context of "one-time" (a.k.a. "dynamic") password generation. Guski, col. 1, lines 40-42. Accordingly, Guski teaches that at the time of password generation, password generator 300 may receive a current time/date and transform that current date/time in order to produce a time sensitive, i.e., one-time, password. Guski, col. 6, line 36-39 ("password generator generates a one-time password 310 as a function of the . . . time/date"). At a different time, password generator 300 receives a different current time and generates a different password. See Guski, col. 9, lines 63-65 ("password for a given user ID and application ID changes every second"). By contrast, in one embodiment of the present invention, the password generation is not time sensitive at all. Present application, page 4 , lines 9-10 ("same password for that application and secret key combination every time"); see also, for example, page 6, lines 4-15 (no time element to password generating components).

In another embodiment of the present invention, the generated password is time dependent, but not in the particular fashion taught by Guski, in which a current time/date is *captured as a time stamp indicating a particular instant in time*, which has nothing to do with user action. See Guski, col., 8, lines 7-12 and col. 9, lines 63-65 (time stamp instant in time changes every second). This time stamp is transformed and incorporated into the generated password. Guski, col. 9, lines 1-8 (XOR operation 416 and encipherment routine 420).

In contrast with the time stamp arrangement taught by Guski, according to a time-dependent password generation embodiment of the present application, a time *interval* may be specified by the user, such as six months or three months, for example. See present application, page 6, lines 17-26 (user specifies six months); and page 12, lines 5-10 (user

Page 12 of 16

specifies three months). That is, in this user-specified-time-interval embodiment of the present invention, within each time interval a password generator generates the same password repeatedly responsive to receiving the same application name, but then, in each succeeding time interval, the password generator generates a new password even though it receives the same application name and uses the same key. See present application, page 6, lines 20-22 (particular combination of key, application name and time period generates the same password "at any time during the period"); page 12, lines 5-10 ("Every quarter, passwords generated by the password generator are different.").

Thus even if the password generator receives an instance of application name at a time 24 hours or more after a earlier instance, if the user has specified no time interval for expiration, i.e., validity, the password generator will generate the same password in both instances. And even if the user has specified a time interval for validity, the password generator will generate the same password in both instances, provided the interval has not elapsed.

Amendments

Claims are amended herein to more particularly point out the novel and nonobvious differences of the present invention as described herein above. No new matter is added, since the original application provides support for the amendments as indicated above.

Claims 1, 18 and 27

Claim 1, for example, is amended herein to state that an inventive method includes "receiving a first application name by the password generator *at a first time* . . . generating a first instance of a first password for said first application . . . based on at least said first application name received at the first time and based on said single key . . . receiving said first application name again . . . *at a second time*; and generating a second instance of the first password based on at least said first application name received at the second time and based on said single key . . ." where "the generated first *password is identical* in its first and second instances if no time interval has been user specified for the first and second instances or if a time interval has been user specified but has not elapsed between the first and second times" (emphasis added). Claims 18 and 27 are herein similarly amended, each according to the form of the invention they respectively claim.

The cited art does not teach or suggest, alone or in combination, that a password generator generates the same password in instances separated in time if no time interval has been user specified or if a time interval has been user specified but has not elapsed between times responsive to receiving the same application name in respective instances.

Claims 2, 19 and 28

Claim 2, for example, is amended herein to state that an inventive method includes "receiving a second application name . . . at a third time . . . generating a first instance of a second password for said second application . . . based on said second application name received at the third time and based on said single key, wherein the *second password is different than the first password . . .*" (emphasis added). And is further amended to state that the method includes "receiving said second application name again at a fourth time . . . and generating a second instance of the second password . . . based on at least said second application name received at the fourth time and based on said single key . . . " where "the generated *second password is identical* in its first and second instances if no time interval has been user specified for the first and second instances or if a time interval has been user specified but has not elapsed between the third and fourth times" (emphasis added). Claims 19 and 28 are herein similarly amended, each according to the form of the invention they respectively claim.

This claim particularly points out that the second of the generated passwords is different than the first, which is due to the receipt of two different application names. In other respects, it makes the same point made by the first claim, which the cited art does not teach or suggest, alone or in combination, i.e., that a password generator generates the same password in instances separated in time if no time interval has been user specified or if a time interval has been user specified but has not elapsed between times responsive to receiving the same application name in respective instances.

Claims 3, 20 and 29

Claim 3, for example, is amended herein to state that an inventive method includes "receiving a *user-specified time interval* . . . indicating a interval *during which the password generator is to produce identical instances* of the first password for identical instances of the received first application name and single key . . ." (emphasis added). Further, the claim is herein amended to state that the method includes "generating a third instance of the first

App. No. 10/734,846   Docket JP920030198US1
Filing Date: 12/12/2003

password . . . responsive to receiving said application name at a time *after expiration of the interval*, wherein in the third instance the generated *first password is different* than the first and second instances of the first password, *even though* the application name received for generating the third instance of the first password is identical to the application name received at the first and second times" (emphasis added). Claims 20 and 29 are herein similarly amended, each according to the form of the invention they respectively claim.

The cited art does not teach or suggest, alone or in combination, receiving a *user-specified time interval during which the password generator is to produce identical instances* of the first password for identical instances of the received first application name and single key. Nor does it teach or suggest that, in contrast to the features claimed in claim 1 (wherein the password generator produces identical instances of the first password for identical instances of the received first application name and single key), the inventive method *also* includes generating a third instance of the first password that is different than the first and second instances of the first password responsive to receiving an application name at a time after expiration of the interval, even though the application name received for generating the third instance of the first password is identical to the application name received at the first and second times.

Claims 4-10, 21-26 and 30-35.

Applicant submits dependent claims 4-10, 21-26 and 30-35 are allowable at least because they depend on respectively allowable independent claims. MPEP 2143.03 ("If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious," citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

REQUESTED ACTIONS

For the reasons explained herein above, Applicant contends that the claims as amended herein are patentably distinct, and hereby requests that Examiner grant allowance and prompt passage of the application to issuance.

Respectfully submitted,

Anthony V. S. England
Attorney for Applicants
Registration No. 35,129
PO Box 5307
Austin, Texas 78763
512-477-7165
a@aengland.com